Taming the Tower of Babel:

Software Assurance Findings Expression Schema (SAFES) Framework

Sean Barnum

Today’s Challenge

- There is no standard reporting format for SwA analysis
  - – Very difficult to combine results of multi-perspective analysis
  - – Very difficult to combine results of multi-tool analysis
  - – Very inefficient for tool vendors looking to integrate results with other tools (very costly and redundant)
  - – Very difficult to trend across assessments from different tools or analysts
  - – Very difficult to automate meta-analysis and the assessment process

SAFES Framework Effort

- Software Assurance Findings Expression Schema (SAFES)

- Phase 1 (v0.1) sponsored by the NSA Center for Assured Software (CAS)
- Objectives:
  - Enable and encourage consistency in software assurance tool and service findings
  - Establish more structured and effectively useful software assurance tool and service results
  - Enable integration of results from multiple software assurance tools and services
  - Enable automated processing of software assurance tool and service results

SAFES Approach

- Community collaboration
- Build from state of the practice
- Enhance with state of the art
- Define a comprehensive schema covering all aspects of software assurance analysis reporting
- Strive for usability, flexibility and extensibility
- Mature towards formalization

SAFES Initial Scope

- In-scope perspectives for initial effort (v0.1):
  - Static source code analysis
  - Static binary code analysis
  - Web application penetration testing
  - Data security analysis
  - Fuzzing
  - Threat modeling
  - Architectural risk analysis
- Some vendors actively collaborating others were passively incorporated

SAFES is a comprehensive and detailed schema

- Info on findings
  - Description
  - Categorization
  - Location
  - Prioritization
  - Correlations
- Info on analysis approach
  - Tool or service
  - Methodology
  - Detection mechanisms
- Info on mitigation
- Info on meta-analysis
- Info on personnel
- Info on application
  - Structure, content & configuration
  - Business/mission and security context
- Info on assurance case
- Info on threat analysis

A Sampling of Potential Use Cases

- Understand the Business Context of application
- Identify risks
- Map technical risks to business context
- Map the application attack surface
- Identify relevant threats
- Inventory and characterize assets
- Create threat model
- Define FISMA security categorization (FIPS-199)
- FISMA Security Planning (SP800-18)
- FISMA Risk Assessment (SP800-30)
- Conduct multi-tool/multi-perspective analysis
- Identify false positives
- Characterize risk
- Prioritize risk

- Correlate findings
- Stitch dynamic & static location results
- Integrate automated and manual analysis
- Reuse common mitigation advice
- Create assessment report
- Create different versions of report
- Define an assurance case for an application
- Create an assurance case compliance report
- Import CWE content into local context
- Identify common finding trends across portfolio by technology context
- Maintain analysis accountability
- Identify trends in tool and rule efficacy
- Mapping between various tool level definitions

SAFES Maturation Paths Beyond v0.1

- SAFES Maturation Paths:
  - Usability: primarily focused on efforts surrounding the schema to make it more usable by the community such as native transforms, tooling, etc.
  - Refinement: primarily focused on improving the quality and coverage of the schema itself with activities such as adding new perspectives, adding new schemas, fixing errors, etc.
  - Formalization: primarily focused on gradually (as quickly as is prudent and accepted by the targeted user community) incorporating in formal standards-based approaches (vocabulary, structure, etc.)

SAFES Status

- v0.1 completed and now available on the SAFES website (www.safes-framework.com)
- Currently working with sponsor to finalize decision of next steps to pursue
- Lining up new supporters/sponsors
- Working with various stakeholders in the community to support their use of SAFES and elicit their collaboration

Potential Next Steps

Priority	Action
Very High	Determine vehicle of publication (IP control)
Very High	Create transforms to and from native schemas
High	Move SAFES to a more stable and permanent website
High	Create comprehensive example
High	Create authoring/editing tooling
High	Create report generation tooling
Moderate	Pilot a real project using SAFES
Moderate	Refine schema to add more tools within the initial scope
Moderate	Refactor schema for efficiency and redundancy reduction
Moderate	Map alignment between SAFES and KDM, ARM, SAEM, etc.
Moderate	Formalize schema infrastructure (e.g. XMI compliant) for improved automation interchange and enabling framework layering
Low	Refine schema to add new tools outside the initial scope